AF ZIW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Jon Nash-Putnam	Date: May 18, 2006
Serial No. 09/915,174	Docket No.
Filed: July 25, 2001	Group Art Unit: 2316
For: SYSTEM AND METHOD FOR INSERTION AND RETRIEVAL OF MICROTHREADS IN TRANSMITTED DATA	Examiner: Ronald Baum

Honorable Commissioner for Patents
Mail Stop: Appeal Brief-Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST TO ACCEPT SUBSTITUTE APPEAL BRIEF

SIR:

This is a request that a substitute Appeal Brief be accepted.

Last night, May 17, 2006, shortly before midnight, I attempted to file an appeal brief for this application electronically through the U.S.P.T.O. EFS system. Unfortunately, the copy of the Appeal Brief uploaded to the EFS site turned out to have been corrupted. I discovered this after I was in the pay fees section of processing. By then, the EFS system would not let me go back and fix the problem. I paid the Appeal Brief filing fee, got a filing confirmation, and then sent an uncorrupted version of the electronic version of the Appeal Brief to the EFS office before midnight (EDT). I then followed up with a second email, also containing an uncorrupted copy of the Appeal Brief with a more thorough explanation ten minutes later. I then called the EFS center today for help. After a lot of work on their part, they had to conclude that they could not help here.

I am therefore submitting a paper copy of the Appeal Brief as a replacement for the corrupted electronic version that I submitted last night. This paper copy is identical to the copy that I emailed before midnight last night.

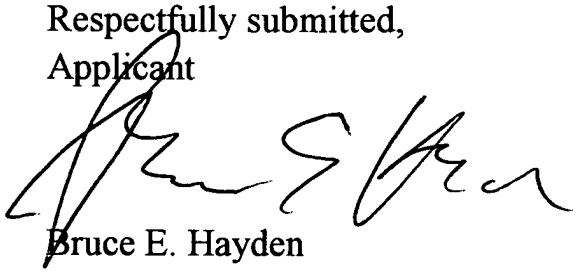
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450 on:

5/18/06 _____
Date Signature Printed or Typed Name

Therefore, please accept the attached Appeal Brief as a substitute for the corrupted Appeal Brief I submitted last night. As can be seen from the attached EFS filing certificate, the Appeal Brief filing fee has already been paid.

Date: May 18, 2006

Respectfully submitted,
Applicant



Bruce E. Hayden
Attorney for Applicants
Registration No. 35,539
Telephone No.
FAX No.

Enc: Appeal Brief
Filing Certificate

Electronic Acknowledgement Receipt

EFS ID:	1050562
Application Number:	09915174
Confirmation Number:	6241
Title of Invention:	System and method for insertion and retrieval of microthreads in transmitted data
First Named Inventor:	Jon Nash-Putnam
Correspondence Address:	Roger W. Westman - 693 Old Squaw Pass Road - Evergreen CO 80439 US 3036790749 roger@westman.cc
Filer:	Bruce Edward Hayden
Filer Authorized By:	
Attorney Docket Number:	015471-0000 - B72625
Receipt Date:	17-MAY-2006
Filing Date:	25-JUL-2001
Time Stamp:	23:38:10
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$ 250

RAM confirmation Number	377
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Appeal Brief Filed	915174Br1.pdf	9069	no	2
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	8170	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	17239		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Jon Nash-Putnam
Serial No. 09/915,174
Filed: July 25, 2001
For: SYSTEM AND METHOD FOR INSERTION AND RETRIEVAL OF MICROTHREADS IN TRANSMITTED DATA

Date: May 16, 2006
Docket No.
Group Art Unit: 2316
Examiner: Ronald Baum

Honorable Commissioner for Patents
Mail Stop: Appeal Brief-Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

SIR:

This Brief is filed pursuant to 37 C.F.R. §41.37 in the matter of the Appeal to the Board of Appeals and Interferences of the rejection of the claims of the above-referenced application for patent.

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450 on

Filed electronically 5/17/06 BLH

5/16/06

Date | Signature | Printed or Typed Name

Real Party in Interest

The real party in interest is 440 Pammel, Inc., a Wyoming corporation, assignee of all rights, title, and interest in this application.

Related Appeals and Interferences

Appellant knows of no related appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-20 are pending in the present application. Claims 1-20 are under active examination and each has been finally rejected. The rejection of each of claims 1-20 is subject to this appeal.

Status of Amendments

A first Office Action on the merits was issued on May 9, 2005. An Amendment was filed in response to the first Office Action on September 12, 2005, with amendments to claims 1-5, 7, 15, 16, and 20. A second Office Action was issued on November 22, 2005, with final rejection of Claims 1-20. No amendments have been filed subsequent to the final rejection.

Summary of Claimed Subject Matter

Claims 1, 7, and 15 are independent claims.

Claim 1 claims a system (104, 106, 108 FIG. 1; ¶¶ 22-41) for the insertion of microthread data in transmitted data (114, 116 FIG. 1; FIG. 2; FIG. 5) comprising: a digital content system (102 FIG. 1) providing carrier data; and a microthread insertion system (114, 116 FIG. 1; FIG.2; FIG. 3; FIG. 7) coupled to the digital content system (102 FIG. 1; ¶¶ 23, 24), the microthread insertion system generating a composite data sequence (FIG. 7) in real-time (¶¶ 22, 28, 36) for transmission that includes the carrier data and the microthread data; wherein the

microthread data is camouflaged in real-time in the composite data sequence using the carrier data (206, 208 FIG. 2; 306 FIG. 3; FIG. 7). (Also see Claim 7 below).

Claim 7 claims a method for inserting microthread data in transmitted data (FIGs. 7, 8, and 11; ¶¶ 70-82, 92-95) comprising the steps of: A) receiving microthread data and carrier data (702 FIG. 7; 802 FIG. 8; 1102 FIG. 11; ¶¶ 70, 78, 92) encrypting the microthread as encrypted microthread data (704 FIG. 7; 1104 FIG. 11; ¶¶ 71, 92); B) camouflaging the encrypted microthread data in real-time (¶¶ 22, 28, 36) using the carrier data to generate camouflaged microthread data (708 FIG. 7; 820 FIG. 8; ¶¶ 72, 81); and C) forming a composite data sequence (720 FIG. 7; 822 FIG. 8; 1110 FIG. 11; ¶¶ 76, 81, 94) in real-time for transmission (724 FIG. 7; 1112 FIG. 11; ¶¶ 76, 94) that includes the carrier data and the camouflaged microthread data. (Also see Claim 1 above).

Claim 15 claims a method for retrieving microthread data from transmitted data (FIGs. 9 and 12; ¶¶ 83-87, 96-101) comprising the steps of: A) receiving transmitted data that is a composite data sequence that includes carrier data and camouflaged microthread data (902 FIG. 9; 1202 FIG. 12; ¶¶ 83, 96); B) locating the camouflaged microthread data in real-time using a flag (1204 FIG. 12; ¶ 97); C) extracting the camouflaged microthread data in real-time (906 FIG. 9; 1206 FIG. 12; ¶¶ 84, 98); and D) extracting the microthread data from the camouflaged microthread data in real-time (908, 910 FIG. 9;1208 FIG. 12; ¶¶ 85, 86, 100).

Grounds of rejection to be reviewed on appeal

Whether the invention of Claims 1-20 is unpatentable under 35 USC § 102(e) as being anticipated by U.S. Patent No. 6,625,295 B1 to Wolfgang, et al. (hereinafter "*Wolfgang*").

Argument

Claims 1-20 were rejected as anticipated under 35 USC § 102(e) by U.S. Patent No. 6,625,295 B1 to Wolfgang, et al. 35 USC § 102(e) states (in relevant part) that: "*A person shall be entitled to a patent unless – (e) the invention was described in - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international*

application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language". However, "*A claim is* ***anticipated*** [under 35 USC § 102(e)] *only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.*" *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) and "*The identical invention must be shown in as complete detail as is contained in the ... claim.*" Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (see also MPEP § 2131).

Rejection of Claim 1

Claim 1 was rejected under 35 USC § 102(e) as being anticipated by Wolfgang. It claims a system for the insertion of microthread data in transmitted data comprising: a digital content system providing carrier data; and a microthread insertion system coupled to the digital content system, the microthread insertion system generating a composite data sequence in real-time for transmission that includes the carrier data and the microthread data; wherein the microthread data is camouflaged in real-time in the composite data sequence using the carrier data.

The rejection in the second Office Action recited: "*A system for the insertion of microthreads [watermark(s)] in transmitted data comprising: a digital content system providing carrier data.4 [figures 1-6 and associated descriptions, abstract, col. 1,lines 25-col. 4,line 67, whereas the watermark generation/insertion and original signal aspects, clearly encompasses the ".. . digital content ... carrier data ...", as broadly interpreted by the examiner]; a microthread insertion system coupled to the digital content system, the microthread insertion system generating a composite data sequence in real-time for transmission that includes the carrier data and the microthread data; wherein the microthread data is camouflaged in real-time in the composite data sequence using the carrier data [figures 1-6 and associated descriptions, abstract, col. 1,lines 25- col. 4,line 67, whereas the watermark generation/camouflaged via encryption (i.e., made visually imperceptible)/insertion and original signal aspects, clearly encompasses the"... microthread insertion ... carrier data ... camouflaged ... carrier data ...", as broadly interpreted by the examiner].*"

First note that the term "*as broadly interpreted by the examiner*" is used on multiple occasions in this rejection. This is a clear indicia that the rejection is actually based on obviousness, and, thus, would more appropriately have been rejected under 35 U.S.C. § 103(a) instead of § 102(3). However, § 102(e) anticipation rejections typically cannot be overcome by secondary indicia of nonobviousness (see MPEP § 2131.04 and 2131.05). So, this assertion that the elements "*as broadly interpreted by the examiner*" is a transparent attempt to bootstrap obviousness analysis into anticipation rejections, without paying the penalty for obviousness rejections of allowing secondary indicia of nonobviousness to overcome the rejection. And, that this was done on multiple occasions in the rejection is significant indicia that the reference indeed does not teach or describe the limitations in the claims.

It should also be noted that the "*microthreads*" the instant invention inserts into and detects in transmitted data differ from the "*watermarks*" utilized in the Wolfgang reference, esp. since the Wolfgang watermarks by necessity are included in much of, and preferably the entirety of, images. For example: "*In one embodiment hereafter referred to as the constant-W two-dimensional watermark (CW2D), the watermark 50 is created by forming an m-sequence and then shaping it to form a block (w) of the watermark. For example, the watermark block is created by forming a 2^{16}-1 period bipolar m-sequence and then shaping the sequence to form a 256 X 256 watermark block (w). To create a block of the watermarked original image (y) a 256 X 256 block of the original image (x) is extracted to which w is added: y=x+w. This process is repeated until the entire image is marked.*" Col. 7, Lines 8-18.

The basic function of the Wolfgang patent was the "*authenticate*" an image. This can be seen from its titled "*Authentication of signals using watermarks*" and its field of invention "*The present invention relates to methods and apparatus for protecting and authenticating information, and particularly to protecting and authenticating information using watermarks. More particularly, the present invention relates to methods and apparatus that determine whether a suspect signal is derived from a watermarked original signal by analyzing the suspect signal for the presence of a known watermark*". The purpose of this authenticatiton is given starting in the first three paragraphs of the Background Section:

> ...Copyright owners need tools for identification content authentication, that is, identification of copies of the protected work that may have been forged, filtered, or otherwise modified, as well as ownership

authentication. It may also be necessary to determine a work's chain of custody and to verify who viewed or altered the work, including when such actions occurred.

Three techniques for protecting information are encryption, authentication, and time stamps. Encryption disguises the content of information so that only users who possess the decryption "key" can convert the encrypted data back to its original form. Without the key, it is computationally infeasible to derive the original data. Another technique is authentication, which does not hide the content of the data but rather guarantees who created it. Time stamps can identify both the time at which the work was generated and the work's owner. All three techniques may be used in various combinations.

Authentication techniques for protecting information can use what is known as a watermark. A watermark can take many forms, such as a change in the thickness of the paper on which information appears or some other physical characteristic of the medium carrying the information, or it can be included as part of the information on the medium. Typical examples are the watermarks included on checks or paper money, which aid in authenticating the item and preventing its forgery. In essence, a watermark is a code or image incorporated onto the carrier of the original information, and can be either visually perceptible or imperceptible.

In short, a "*watermark*" as used in Wolfgang is a code or image incorporated into data in order to allow the data to be authenticated. The patent then proceeds to provide a method of authenticating data without the necessity of decoding or isolating the watermark in suspect data. The contents of a watermark itself are irrelevant in Wolfgang because its whole purpose is to provide a mechanism for not having to separate a watermark from the data in which it is embedded in order to determine whether or not it is present.

The "*microthreads*" disclosed in the present invention are significantly different. Their purpose is to transmit information. This is evidenced by the various types of microthreads shown in the disclosure, such as: "*date and time stamp data, quality of transmission data (such as data that is used to determine whether the transmission quality meets minimum predetermined criteria), advertiser identification data, broadcaster identification data, transmitter identification data, or other suitable data*" (¶ 28), "*broadcast date and time stamp data, copyright data, station identification data, quality of transmission data, or other suitable*

data" (¶ 30), "*a unique transaction code, authentication code, verification code, or other suitable reference key to a data record resident at the correction/probation facility, state or federal human services facility, service provider, client site, or other suitable locations*" (¶ 40), and "*verification of receipt data, advertising data, date and time stamp data, quality of transmission data, broadcaster identification data, or other suitable data*" (¶ 43).

In other words, *microthreads* have value and provide information, in and by themselves, to the recipient of a transmission, whereas the only value of the *watermarks* in the Wolfgang reference is to prove the authenticity of the data in which they are embedded. One may think of it this way. In both cases, there is underlying data (D) in which other data (I) is inserted. The purpose of the *watermarks* (I) in the Wolfgang reference is solely to prove the authenticity of the data (D), and for that reason, the recipient of the combined signal (D+I) never sees the content of a *watermark* (I). Rather, the authentication is performed by comparing $f((D+I)_0)$ with $f((D+I)_1)$, where $(D+I)_0$ is a base copy of the combined signal, and $(D+I)_1$ is a received copy. But the present invention combines (D)+(I)=(D+I) in *real-time* (see below), transmits the combined signal (D+I), and then separates them (D+I)=(D)+(I) into their components (D) and (I), for the express purpose of transmitting hidden information through the *microthreads* (I). Wolfgang *watermarks* are thus significantly different from the *microthreads* disclosed in the present invention, and, thus, are an element missing from the Wolfgang reference.

Nevertheless, the claims were amended in response to the first Office Action to include a limitation that the insertion be done in "*real-time*" in order to more clearly distinguish the present invention from the Wolfgang reference. The Wolfgang reference does not insert its watermarks in "*real-time*". Rather, it inserts its watermarks into images "*off-line*". This means that it inserts them into an image, and, later, the image is transmitted. It is, by necessity, in that reference, a two step process. For example, "*One aspect of the present invention provides for authenticating whether suspect information contains the original, protected information by incorporating a watermark onto the original information before making it available over network 22*", Col. 5 Lines 61-65. The "*watermarked original image*" 56 is then at some later point transmitted. Indeed, it may be transmitted many times. And then, later, the "*watermarked original image*" 56 is utilized for comparison with a received image. This is clearly not done in real-time, and is not done for immediate, *real-time*, transmission. (see FIG. 2 of the present

invention and associated discussion below). Inserting watermarks *off-line*, instead of in *real-time*, is crucial to the Wolfgang invention.

Contrast this with the present invention. For example, in the case of audio (radio) broadcasts, the live broadcast signal is dynamically modified in *real-time* to include the microthreads, such as "*broadcast verification data*" (see ¶ 6). "*The microthread data can include data used to verify receipt of the carrier data, date and time stamp data, quality of transmission data (such as data that is used to determine whether the transmission quality meets minimum predetermined criteria), advertiser identification data, broadcaster identification data, transmitter identification data, or other suitable data*" (see ¶ 28). Much of this data cannot be inserted *off-line*, as is done with static data in Wolfgang, because, for example, it is live, *real-time*, data. It only makes sense when inserted *real-time* as part of the transmission process.

The fundamental difference here is that *off-line* insertion done in Wolfgang separates the insertion in time and space from the transmission of the data in which it is embedded. It is necessary that it is done this way in Wolfgang in order to retain an image with the embedded watermark ($(D+I)_0$ above) for later comparison with received a received image ($(D+I)_1$). The *real-time* insertion claimed here is done as part of the transmission process.

It should be noted that both of the other two cited references, Shumann et al., U.S. Patent No. 6,285,774 and Ezaki et al., U.S. Patent No. 6,721,437 B1, appear to operate in a similar manner to Wolfgang, with *off-line* and not *real-time* watermark insertion. Indeed, Schumann is titled "*System and methodology for tracing to a source of unauthorized copying of prerecorded proprietary material, such as movies*", which is strong indicia that the "*running marks*" it utilizes are inserted *off-line*. And while the Ezaki reference at first glance (see FIG. 8, "*Electronic Watermark Embedding Section*") appears from the drawings to show the embedding of watermarks in *real-time*, there is no mention of how that could be done. Rather, the reference is devoted entirely to the "*reception side*", leaving the "*transmission side*" to the prior art. And, indeed, the type of watermark being decoded by Ezaki is invariably decoded "*off-line*" and not in "*real-time*" in the prior art.

Applicant respectfully submits that the cited Wolfgang reference does not disclose several elements present in the rejected claims, including the use of microthreads and the insertion of microthreads in real-time. They are also not present in either of the other two references mentioned by the Examiner. Reference

to quasi-obviousness analysis through the repeated use of "*as broadly interpreted by the examiner*" does not overcome these failings, since the differences are significant, and this is an anticipation rejection (§ 102(e)), not a nonobviousness rejection (§ 103(a)). Indeed, the repeated use of this term is indicia that the Wolfgang does not include significant elements and limitations of the rejected claim. For these reasons, Applicant respectfully requests that the rejection under 35 U.S.C. § 102(e) of this claim, as well as others referencing this argument, as anticipated by Wolfgang be withdrawn.

Rejection of Claim 2

Claim 2 is dependent upon claim 1 and the arguments for overcoming the rejection of that claim are incorporated herein. However, it also included the additional limitation of "*a key encryption system encrypting the microthread data prior to forming the composite data sequence*". This claim was also rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. The second Office Action rejected this additional limitation based first on the argument that Wolfgang made watermarks visually imperceptible via encryption. While that alone is a highly questionable definition of the term "*encryption*", more importantly, the hiding of watermarks in data in Wolfgang is not "*key encryption*". That is a term of art, and identifies one type of *encryption*. Wolfgang utilizes a different type of *encryption*, if you can even use that term for what the reference discloses (which is highly questionable).

Note the text from the second paragraph of the Background Section of Wolfgang quoted above which distinguished between encryption, authentication, and time stamps. Wolfgang, by its Title, Field of Invention, Summary, Claims, etc. was concerned solely with "*authentication*", and, thus, not "*encryption*". Use of the terminology (again) of "*as broadly interpreted by the examiner*" cannot change the fact that Wolfgang started out by essentially saying that: *There are three primary ways of authenticating data, X, Y, and Z. This invention involves Y.* The "*as broadly interpreted by the examiner*" can't make Y (authentication) into X (encryption), as was argued in the Office Action. As that paragraph points out, they are two different and distinct approaches for solving the same problem.

For all the reasons above, the Applicant respectfully submits that there are significant additional limitations found in this claim that are not found in the Wolfgang reference, and therefore requests that the rejection of this claim as anticipated by Wolfgang be withdrawn.

Rejection of Claims 3, 5, 6

Claims 3, 5, and 6 were rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. All these claims are dependant, directly or indirectly, on claim 1, and, therefore, the arguments for overcoming the rejection of claim 1 are incorporated herein by reference. For that reason, Application respectfully submits that the rejection of these claims is incorrect, and requests that it be withdrawn.

Rejection of Claim 7

Claim 7 was rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. The second Office Action asserted that it was the method claim equivalent of combining claims 1 and 2. While there are some differences, Applicant does not view them as significant. Therefore, the arguments above for claims 1 and 2 are incorporated herein by reference, and Applicant respectfully requests that the rejection of this claim under 35 U.S.C. § 102(e) as being anticipated by Wolfgang be withdrawn.

Rejection of Claims 4 and 8

Claims 4 and 8 were rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. Claim 4 is dependent upon Claim 1, and Claim 8 is dependent on Claim 7, and the arguments for the underlying claims are incorporated herein by reference.

They also include the limitation of "*a carrier length system determining whether the carrier data is long enough to carry the microthread data and duplicating the carrier data if the carrier data is not long enough*". The Office Action cited instances in the Wolfgang reference where the watermark is duplicated to fill the image being watermarked. But this is the opposite of what is being claimed. Here, the carrier is padded to be long enough to accommodate the microthread. This is a significant additional limitation not found in Wolfgang.

Therefore, for the reasons cited above, Applicant respectfully submits that the rejection of these claims under 35 U.S.C. § 102(e) as anticipated by Wolfgang is inappropriate, and requests that it be withdrawn.

Rejection of Claims 9, 10, 11, 12, and 13

Claims 9 through 12 were rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. All these claims are dependant, directly or indirectly, on claim 7, and, therefore, the arguments for overcoming the rejection of claim 7 are

incorporated herein by reference. For that reason, Application respectfully submits that the rejection of these claims is incorrect, and requests that it be withdrawn.

Rejection of Claim 14

Claim 14 was rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. It is indirectly dependant upon claim 7, and, therefore the arguments for overcoming the rejection of that claim are incorporated herein by reference. This claim further includes a limitation that: "*the predetermined data sequence of the carrier data is a predetermined magnitude of change in two successive data values*". This is not defined in detail in the claim, and, therefore, the Office Action again uses "*as broadly interpreted by the examiner*" to greatly expand what is disclosed in Wolfgang to reject this claim. However, the methodology being claimed is defined in the specification describing FIGs. 7 and 8 (starting at ¶ 70) involving "*lossy*" data. Lossy data is most often analog at some point. During transmission, digital data is converted to analogue, and converted back during reception. This is typically done through digital/analog (D/A) and analog/digital (A/D) conversion. This is extremely well known in the art, and is the basis of much of our communications technology today. The digital data that is translated to/from analog typically consists of an ordered series of numerical values. For example, in ¶ 73, "*In one exemplary embodiment, the carrier data can be digitally sampled audio data or other suitable digitally encoded analog data. An insertion point can be determined by locating two successive values of sequential carrier data that have an absolute magnitude difference greater than a predetermined value*". An engineer reasonably competent in the relevant art can easily determine the meaning of this methodology step.

Contrast this, however, with Wolfgang. Though that reference does not specifically use the term, it is entirely dedicated to "*lossless*" data transmissions, which are the opposite of "*lossy*" data transmissions, as is discussed in these FIGs. 7 and 8. These two terms are well known in the art. Examples given in the specification for *lossy* data include "*sampled audio or video data*", whereas *lossless* data includes "*TCP/IP format data*" (¶ 26). Since this claimed methodology is most useful for, and described in relation to, lossy data transmissions, and Wolfgang is limited to lossless data transmissions, vague "*as broadly defined by the examiner*" reasoning is clearly insufficient to anticipate this claim element.

For the reasons discussed here and above, Application respectfully submits that the rejection of this claim under 35 U.S.C. § 102(e) as being anticipated by Wolfgang is incorrect, and requests that it be withdrawn.

Rejection of Claim 15

Claim 15 was rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. The Office Action rejected this claim arguing that "*this claim is the "receive and recover/verify" side of the claim 7 "create thread/watermark, insert, transmit" limitations above, and is rejected for the same reasons provided for the claim 7 rejection*". Applicant therefore incorporates by reference his arguments concerning claims 1 and 7 above.

However, the claim is "*A method for retrieving microthread data from transmitted data comprising: receiving transmitted data that is a composite data sequence that includes carrier data and camouflaged microthread data; locating the camouflaged microthread data in real-time using a flag; extracting the camouflaged microthread data in real-time; and extracting the microthread data from the camouflaged microthread data in real-time*".

One major problem with the rejection is that it facilely combines "*recover/verify*" as one element. But these are distinct. Wolfgang teaches *verification*, and this claim claims *recovery* or *extraction*. Indeed, the avowed purpose of Wolfgang is to validate received data containing watermarks without the necessity of recovering the embedded watermarks.

Thus, Wolfgang, no matter how broadly it is interpreted by the examiner, does not teach "*extracting the camouflaged microthread data*". And note, that it also is not extracted in real-time.

Claim 15 has significant elements that are not shown in the Wolfgang reference. Therefore, for the reasons cited above, and for this reason, Applicant respectfully submits that the rejection of this claim under 35 U.S.C. § 102(e) as being anticipated by Wolfgang is incorrect, and requests that it be withdrawn.

Rejection of Claims 16 through 20

Claims 16 through 20 were rejected under 35 U.S.C. § 102(e) as being anticipated by Wolfgang. All these claims are dependant, directly or indirectly, on Claim 15, and, therefore, the arguments for overcoming the rejection of Claim 16 are incorporated herein by reference. For that reason, Application respectfully

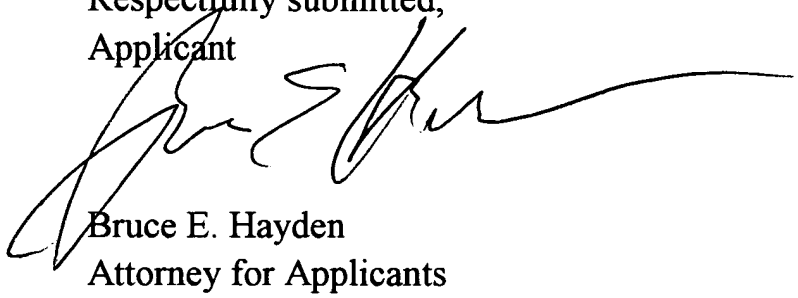
submits that the rejection of these claims is incorrect, and requests that it be withdrawn.

Conclusion

Reversal of the final rejections of Claims 1-20 is respectfully requested in view of the foregoing arguments.

Date: May 16, 2006

Respectfully submitted,
Applicant



Bruce E. Hayden
Attorney for Applicants
Registration No. 35,539
Telephone No.
FAX No.

Appendix of Claims Involved in Appeal

1. A system for the insertion of microthread data in transmitted data comprising:
a digital content system providing carrier data; and
a microthread insertion system coupled to the digital content system, the microthread insertion system generating a composite data sequence in real time for transmission that includes the carrier data and the microthread data;
wherein the microthread data is camouflaged in real time in the composite data sequence using the carrier data.

2. The system of claim 1 wherein the microthread data insertion system further comprises:
a key encryption system encrypting the microthread data prior to forming the composite data sequence.

3. The system of claim 1 wherein the microthread data insertion system further comprises:
a camouflage system receiving the microthread data and the carrier data and performing a mathematical operation using the microthread data and the carrier data to generate camouflaged microthread data.

4. The system of claim 1 wherein the microthread data insertion system further comprises:
a carrier length system determining whether the carrier data is long enough to carry the microthread data and duplicating the carrier data if the carrier data is not long enough.

5. The system of claim 1 wherein the microthread data insertion system further comprises:
a camouflaged microthread insertion system receiving the microthread data and inserting the microthread data into the carrier data at one or more locations.

6. The system of claim 3 wherein the camouflage system further comprises a difference system generating camouflaged microthread data by generating two successive sections of carrier data having a difference equal to an integer times the microthread data.

7. A method for inserting microthread data in transmitted data comprising:
receiving microthread data and carrier data;
encrypting the microthread as encrypted microthread data;
camouflaging the encrypted microthread data in real time using the carrier data to generate camouflaged microthread data; and
forming a composite data sequence in real time for transmission that includes the carrier data and the camouflaged microthread data.

8. The method of claim 7 wherein receiving the carrier data further comprises:
determining a length of the carrier data; and duplicating the carrier data until the length of the duplicated carrier data is long enough to carry the microthread data.

9. The method of claim 7 wherein camouflaging the microthread data using the carrier data comprises
performing a mathematical operation using the encrypted microthread data and the carrier data.

10. The method of claim 7 wherein camouflaging the microthread data using the carrier data comprises
generating two successive sections of carrier data having a difference equal to an integer times the microthread data.

11. The method of claim 7 wherein camouflaging the microthread data using the carrier data comprises
storing the microthread data in one or more predetermined data frame locations.

12. The method of claim 7 wherein forming the composite data sequence that includes the carrier data and the camouflaged microthread data comprises:
storing the microthread data and locator data in a first data frame location;
using the locator data to determine a second data frame location; and
storing the microthread in the second data frame location.

13. The method of claim 7 wherein forming the composite data sequence that includes the carrier data and the camouflaged microthread data comprises
storing the camouflaged microthread data at one or more predetermined locations based on a predetermined data sequence of the carrier data.

14. The method of claim 13 wherein the predetermined data sequence of the carrier data is a predetermined magnitude of change in two successive data values.

15. A method for retrieving microthread data from transmitted data comprising:
receiving transmitted data that is a composite data sequence that includes carrier data and camouflaged microthread data;
locating the camouflaged microthread data in real time using a flag;
extracting the camouflaged microthread data in real time; and
extracting the microthread data from the camouflaged microthread data in real time.

16. The method of claim 15 further comprising
performing one or more predetermined actions in real time using the microthread data.

17. The method of claim 15 wherein locating the camouflaged microthread data using the flag comprises locating a predetermined characteristic of the carrier data.

18. The method of claim 17 wherein the predetermined characteristic is a change in two successive values of data that exceeds a predetermined amount.

19. The method of claim 17 wherein the predetermined characteristic is a data frame location.

20. The method of claim 15 wherein extracting the microthread data from the camouflaged microthread data comprises performing a mathematical operation on the camouflaged microthread data.

Evidence Appendix

None

Related Proceedings Appendix

None